

PRESENTATION

Legal Issues Confronting Inside Counsel

Tuesday, November 17, 2015

BAKER DONELSON

EXPAND YOUR EXPECTATIONS™

Mark Glover

Shareholder

Baker Donelson

Attorney-Client Privilege as Applied to In-house Counsel

Attorney-Client Privilege in General

- No reference to, or “grant” of the privilege in either the U.S. Constitution or the Federal Rules of Evidence
- Considered a creature of state law or federal common law and therefore differs from jurisdiction to jurisdiction in minor respects
- The case commonly cited for articulation of the definitive elements of the attorney-client privilege is ***United States v. United Shoe Machinery Corp.***, 89 F. Supp. 357 (D. Mass. 1950)

The Rule

- A party seeking to invoke the privilege has the burden of establishing its existence and generally must show that:

(1) the asserted holder of the privilege is or seeks to become a client; (2) the person to whom the communication was made (a) is a member of the bar of a court, or his subordinate and (b) in connection with this communication is acting as a lawyer; (3) the communication relates to a fact of which the attorney was informed (a) by his client (b) without the presence of strangers (c) for the purpose of securing primarily either (i) an opinion on law or (ii) legal services or (iii) assistance in some legal proceeding, and not (d) for the purpose of committing a crime or tort; and (4) the privilege has been (a) claimed and (b) not waived by the client.

89 F. Supp. 357,358 (D. Mass. 1950)

Shorthand Rule

- Communication
- Between counsel and client
- Made confidentially
- For the purpose of obtaining legal advice

Purpose of the Privilege

- To encourage full and frank communications between attorneys and their clients. The courts recognize that sound legal advocacy serves public interest and that sound advice or advocacy depends upon the attorney being fully informed by the client.
- All well-reasoned opinions analyze the issue of whether the privilege exists in the context of this purpose.

Burden of Establishing the Privilege

Unlike the work-product doctrine, which allows a court to order discovery where the party seeking discovery shows that it has a “substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means”...The attorney-client privilege works as an absolute bar to discovery where the privilege exists.

So...

The party asserting it has the burden of proving the privilege exists.

And...

Courts generally construe the privilege narrowly and it can be waived, sometimes even inadvertently.

Upjohn

In 1981, the Supreme Court formally extended the attorney/client privilege to in-house counsel.

Upjohn Co. v. United States, 449 U.S. 383 (1981).

Questions of privilege are more complex in the corporate setting because a corporation is an “artificial creature of the law and not an individual...”

Upjohn at 389-90.

Two Questions Arise

1. When is an individual within a corporation a “client” for purposes of applying the privilege?
2. Is counsel acting predominantly in a business capacity or in a legal capacity in the communication at issue?

Who is the In-House Attorney's Client?

Answer: The corporation (but when is a corporate employee entitled to expect confidentiality when dealing with in-house counsel?)

Courts have employed a variety of tests:

- Corporate control test
- Subject matter test
- *Upjohn* test

The *Upjohn* Test (majority)

The privilege protects communications between in-house counsel and a corporation's employee if:

- Corporate employees have made a communication to in-house counsel “ACTING AS SUCH” for the purpose of seeking legal advice for the corporation.
- The subject of the communication must involve matters that are within the scope of the employee's corporate duties.
- The employees themselves are clearly aware that their statements are being provided for the purpose of obtaining legal advice for the corporation.
- The communication is confidential when made and is kept confidential by the company.

Control Test

- Minority of jurisdictions employ it.
- Still stuck in the mind of some judges and may influence their ruling.
- Restrictive test.
 - Only extends protected communication to the corporation's controlling executives and to those who play a major role in making decisions based upon the in-house attorney's advice. ***City of Philadelphia v. Westinghouse Elec. Corp.***, 210 F. Supp. 483, 485 (E.D. Penn. 1962).

Subject Matter Test

- Focuses the inquiry on whether an employee's communications with in-house counsel are "at the direction" of his or her superiors, AND the "subject matter" of the communication is related to the performance by that employee of his/her corporate employment duties. ***Harper & Rowe Publishers, Inc. v. Decker***, 423 F.2d 487 (7th Cir. 1970).
- Many courts have merged the ***Upjohn*** test with elements of the subject matter test.

Tennessee

- Tennessee state courts have not formally adopted a specific test.
- No statute controls “in-house” issues per se.
- Tennessee courts look to federal court holdings and the positions of other jurisdictions.
- There is no presumption that an in-house attorney’s mere presence at meetings or inclusion on written communications with corporate representatives renders the communications privileged.

-
- ***Leazure v. Apria Healthcare, Inc.***, 2010 WL 3895727 (E.D. Tenn. Sept. 30, 2010)
 - The District Court for the Eastern District of Tennessee “predicted” Tennessee state courts’ stance on in-house attorney-client privilege:

“It is now generally accepted that communications between an attorney and client of primarily a business nature are outside the scope of the privilege. The issue of the principle nature of the advice given by the attorney, i.e., business or legal, most often arises when in-house counsel offers advice to its corporate employer.”

I could find no Tennessee decision which squarely addresses the issue of the attorney-client privilege as it applies to in-house counsel who perform different functions within a corporation. However, the [cited] cases . . . focus on the primary nature of the communications between client and attorney to determine if the communications are privileged [and] comport seamlessly with the purpose of the attorney-client privilege under Tennessee law: ‘the purpose of the privilege is to shelter the confidences a client shares with his or her attorney when seeking legal advice, in the interest of protecting a relationship that is a mainstay of our system of justice.’ . . . Accordingly, . . . a communication between a client and his attorney which serves primarily a business or administrative purpose as opposed to providing legal advice is a communication not protected by the attorney-client privilege.”

Leazure at *1-2 (internal citations omitted) (emphasis added).

Additional Tennessee Guidance From Federal Courts

- ***Edwards v. Whitaker***, 868 F. Supp. 226 (M.D. Tenn. 1994).

“[T]he [attorney-client] privilege only applies if the lawyer is providing legal advice or services, and it will not protect disclosure of non-legal communications where the attorney acts as a business or economic advisor.”

Id. at 228.

-
- ***In re S. Industrial Banking Corp.***, 35 B.R. 643 (Bankr. E.D. Tenn. 1983)

“the involvement of an attorney in the commercial endeavors of a corporation does not per se vitiate the attorney-client privilege, . . . the participation of general counsel in the business of the corporation likewise does not automatically cloak the business activity with the protection of the attorney-client privilege.”

Id. at 647.

The Legal Advice Must Predominate

- ***Alomari v. Ohio Dep't of Pub. Safety***, 2013 WL 5180811 (S.D. Ohio Sept. 13, 2013)

“Where business and legal advice are intertwined, the legal advice must predominate for the communication to be protected.”

Id. at *2.

- ***N. Am. Mortgage Investors v. First Wis. Nat'l, Bank of Milwaukee***, 69 F.R.D. 9 (E.D. Wis. 1975)

“For the privilege to exist, the lawyer must not only be functioning as an advisor, but the advice must be predominately legal, as opposed to business, in nature.”

Id. at 11.

-
- ***Amway Corp. v. Proctor & Gamble Co.***, 2001 WL 1818698 (W.D. Mich. Apr. 3, 2001)

“Where in-house counsel is one of many recipients of a memo, a heavy burden exists to show a predominately legal purpose.”

Id. at *5.

The Presumption Is That The Communication Is More Likely Business Than Legal

- In *Lindley v. Life Investors Insurance Company of America*, 267 F.R.D. 382, 389 (N.D. Okla. 2010), the court held that, while communications with outside counsel benefit from the presumption that the communications are privileged, communications with in-house counsel are presumed to be “more likely business than legal in nature.”
- Notwithstanding that attitude of the courts, the presumption is rebuttable.
- What factors is a court likely to consider?

Lindley Factors

- (1) If the attorney is providing business advice to the client, even if resulting from a confidential request, no attorney-client privilege attaches to the communication.

- (2) If an attorney is providing legal advice to the client at the client's request, the attorney-client privilege protects the confidentiality of the client's communication as well as the legal advice as it pertains to the client's confidential communication.

- (3) If the communication involves both business and legal issues, the court must determine the primary or predominant purpose of the communication.

-
- (a) If primarily a business purpose, the privilege does not attach and the document must be produced.
 - (b) If primarily a legal purpose and the business portions of the document or communication are distinct and severable and their disclosure would not indirectly reveal the substance of the protected legal portion, the document – redacted of the privileged portions – should be produced.
 - (c) Where, however, the legal and business purposes of the communication are inextricably intertwined, the entire communication is privileged only if the legal purpose outweighs the business purpose.

Lindley at 391.

Factual Context For “Business” v. “Legal” Determination

- ***Visa U.S.A., Inc. v. First Data Corp.***, 2004 WL 1878209 (N.D. Cal. Aug. 23, 2004)
- ***Craig v. Rite Aid Corp.***, 2012 WL 426275 (M.D. Pa. Feb 9, 2012)
- ***In re Grand Jury Subpoena Duces Tecum Dated Sept. 15, 1983***, 731 F. 2d 1032 (2d Cir. 1984)
- ***Puckett v. Arvin/Calspan Field Services, Inc.***, 1986 WL 16714 (6th Cir. 1986)
- ***Georgia Pacific Corp. v. GAF Roofings Manufacturing Corp.***, 1996 WL 29392 (S.D.N.Y. Jan. 25, 1996)
- ***Rusnak v. Dollar General Corp.***, 2005 WL 2840740 (S.D. Ohio 2005)

Increase Your Chance Of Prevailing On Challenges To A Claim Of Privilege

- Label communications where the corporation expects and desires that the privilege attach.

Ex: “Request for Facts to Enable Counsel to Give Legal Advice”

“For The Purpose of Receiving Legal Advice”

“Facts Sought In Anticipation of Legal Action”

“Attorney-Client Privileged Communication”

-
- Segregate legal and business advice into separate communications.
 - Use appropriate title (and consider dropping business title).
 - Describe the legal considerations involved. (Make clear why the information is sought.)

Miscellaneous

- Failure to maintain active bar membership
- Internal corporate investigations
- Corporate waiver of privilege at government request – implications
- Avoid making in-house counsel a witness
 - Offer letters
 - Employment agreements
 - Non-competes
 - Harassment investigations

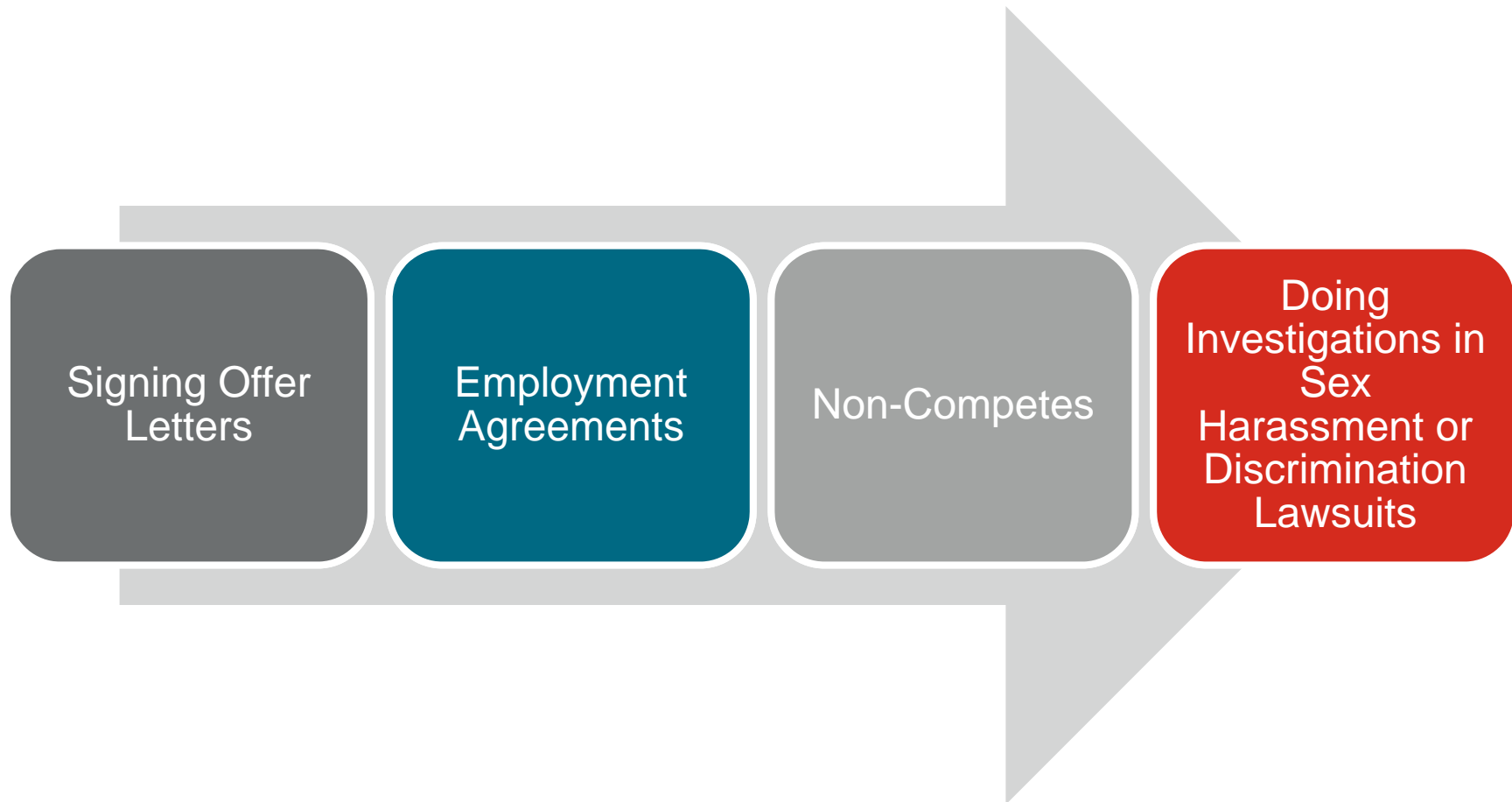
Angie Davis

Shareholder

Baker Donelson

Hot Topics in Employment Law

How to Avoid Making Your In-House Counsel Witness to a Lawsuit



Wage & Hour

Jack In The Box Restaurant Chain Hit With OT Class Action

A former Jack In The Box store manager hit the restaurant chain with a putative class action in California state court on Monday, claiming he was deprived of overtime wages despite regularly working more than 72 hours a week.

Urban Outfitters Inks \$5M Deal With Employees In OT Row

Amazon Workers Seek Approval Of \$3.7M Wage-And-Hour Deal

TWC To Pay \$3.5M To Settle Technician Wages Class Action

Time Warner Cable agreed Friday to pay \$3.5 million to settle a putative class action filed by field service technicians in California who alleged the company failed to pay overtime and minimum wages or to timely pay at termination in violation of the state's labor law.

Panera Hit With \$32M Wages Action Over Meetings, Breaks

Kraft Agrees To \$1.75M Deal To End Unpaid Wages Row

Kraft Foods Group on Wednesday agreed to a \$1.75 million settlement with a putative class of employees who claimed in California federal court they weren't adequately compensated for missed meal and rest breaks.

Wage and Hour

Increase in Collective Action Litigation Under the Fair Labor Standards Act

- Misclassification (exempt/ non-exempt)
- Working off the clock
- Meal/ rest breaks
- Employee/ independent contractors

Damages/ Burdens of Proof

- 2 year/ 3 year look back period
- Record keeping
- Attorneys fees

Department of Labor/Changes to the Salary Basis Test

White Collar Changes
– Executive/
Administrative and
Professional
Employees

New regulation will
eliminate the exempt
status for
approximately 21.4
million employees

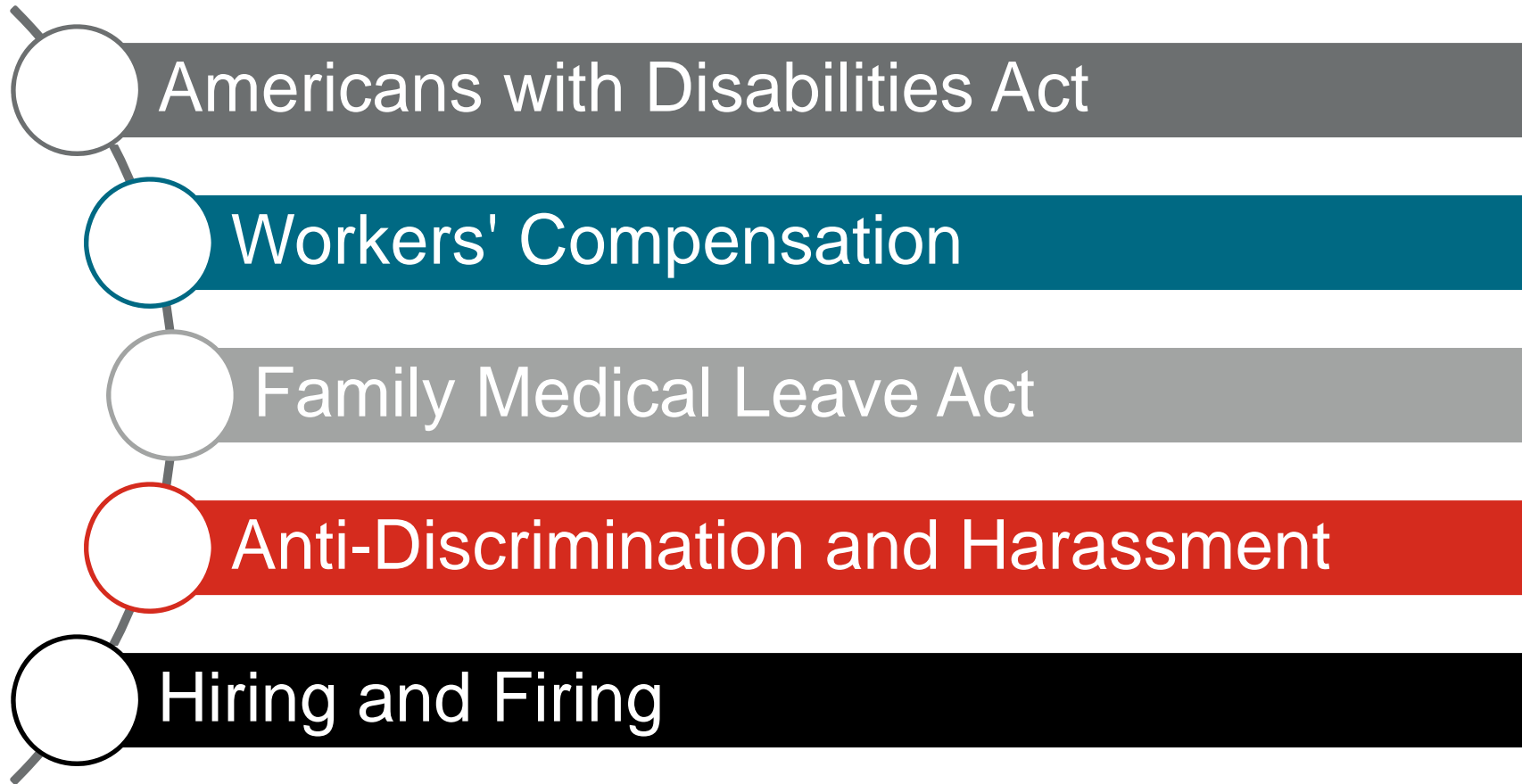
More than doubles the
annual salary required
for employee to be
considered “exempt”

\$23,660 annually to
\$50,440 annually

Less than 90 days to
comply (estimated)

Consider Audit!

Train Employees



Odds and Ends

Reductions In Force

- Labor and employment issues are increasing as downsizing due to the economy is forcing layoffs
- Don't use a position elimination or a Reduction In Force to terminate an employee for poor performance

Immigration/ I-9 Compliance

- Complete I-9 – first day of work
- Review ORIGINAL documents/ copy
- Complete section 2 within 3 days
- Retain I-9s together – ***not in personnel files***
- Consider E-Verify – required in certain industries/ states

Background Checks

- Business related/ job necessity
- Ban the box

George T. (Buck) Lewis

Shareholder

Baker Donelson

Pros and Cons of Arbitration

Possible **Pros** of Arbitration

- Speed of resolution
- Reduced costs
- Arbitrators with specialized expertise
- Privacy/lack of transparency
- Forum selection
- Selection of arbitrator or method of selection
- Elimination/mitigation of class action risks
- Arbitration with non-signatories
- Limited future precedential impact

Possible **Cons** of Arbitration

- Filing fees and arbitrators' fees
- Lack of discovery
- No appeal and VERY limited review of arbitrator decision and conduct
- Privacy/lack of transparency
- Ease of filing for multiple plaintiffs
- Ease of filing and maintenance of baseless claims compared to federal standard under *Twombly*
- Difficulty of getting quick equitable relief such as TROs and temporary injunctions. (See handouts re Interim Measures and Emergency Measures in AAA rules.)

Possible **Cons** of Arbitration (continued)

- Possibility of simultaneous litigation and arbitration
- Possibility of litigation, including appellate litigation, over arbitrability issues under FAA and TAA
- Uncertainty regarding procedural and evidentiary issues due to lack of clear rules and precedent
- Lack of recourse if arbitrators do not follow the law
- Arbitration with non-signatories
- Limited precedential impact

Checklist for Arbitration Agreement and Examples of Agreements

- Method of selection
- Arbitrator qualifications and location
- Location of hearing
- Governing law on primary dispute and arbitrability
- Conditions precedent such as mediation (see new AAA Commercial rule 9.)
- Preliminary relief, interim measures, emergency measures under AAA rules
- Consolidation
- Document discovery and production including electronically stored information
- Deposition limitations and scope of use

Checklist for Arbitration Agreement and Examples of Agreements (continued)

- Duration of matter and length of multiple hearings if necessary
- Limitation upon remedies such as punitive damages, specific performance, and damages caps
- Baseball arbitration
- Attorneys' fees
- Reasoned opinion
- Confidentiality
- Contractual limitations periods and tolling of limitations periods during mediation

Questions?



Kristine L. Roberts

Shareholder

Baker Donelson

Cybersecurity and Management of Electronically-Stored Information

What is Cybersecurity?

Cybersecurity = the process of protecting information by preventing, detecting, and responding to cyber attacks and threats

Why should you be concerned?

Questions from your board and management team

Compliance audits

Government investigations and enforcement actions

Class action lawsuits

Customer demands and expectations

Case study – Target

Hacker used a vendor's access to Target's system to place malware on point-of-sale registers that captured credit and debit card information.

- Fazio Mechanical Services, an HVAC vendor to Target, was authorized to submit billing and project management information to Target
- Fazio was the victim of a phishing email containing malware, which was used to install other malware in Target's network.

Computer security system alerted IT team to suspicious activity, but the team determined it did not warrant immediate follow-up.

Massive data breach:

- Credit and debit card information of 40 million customers
- Personal information (such as addresses) of 70 million customers

Impact of the Target Breach

- Significant hit to sales
- CEO and senior technology executive resigned
- Congressional hearings and government investigations (SEC, FTC)
- Claims by the payment card networks
 - \$67 million settlement with Visa in August 2015
- More than 100 lawsuits
 - Class action that settled for \$10 million (up to \$10,000 per class member)
 - Final approval hearing on November 10, 2015
 - Derivative action against directors and officers
- Costs
 - \$264 million as of 10Q filed August 1, 2015 (offset by \$90 million from insurers)

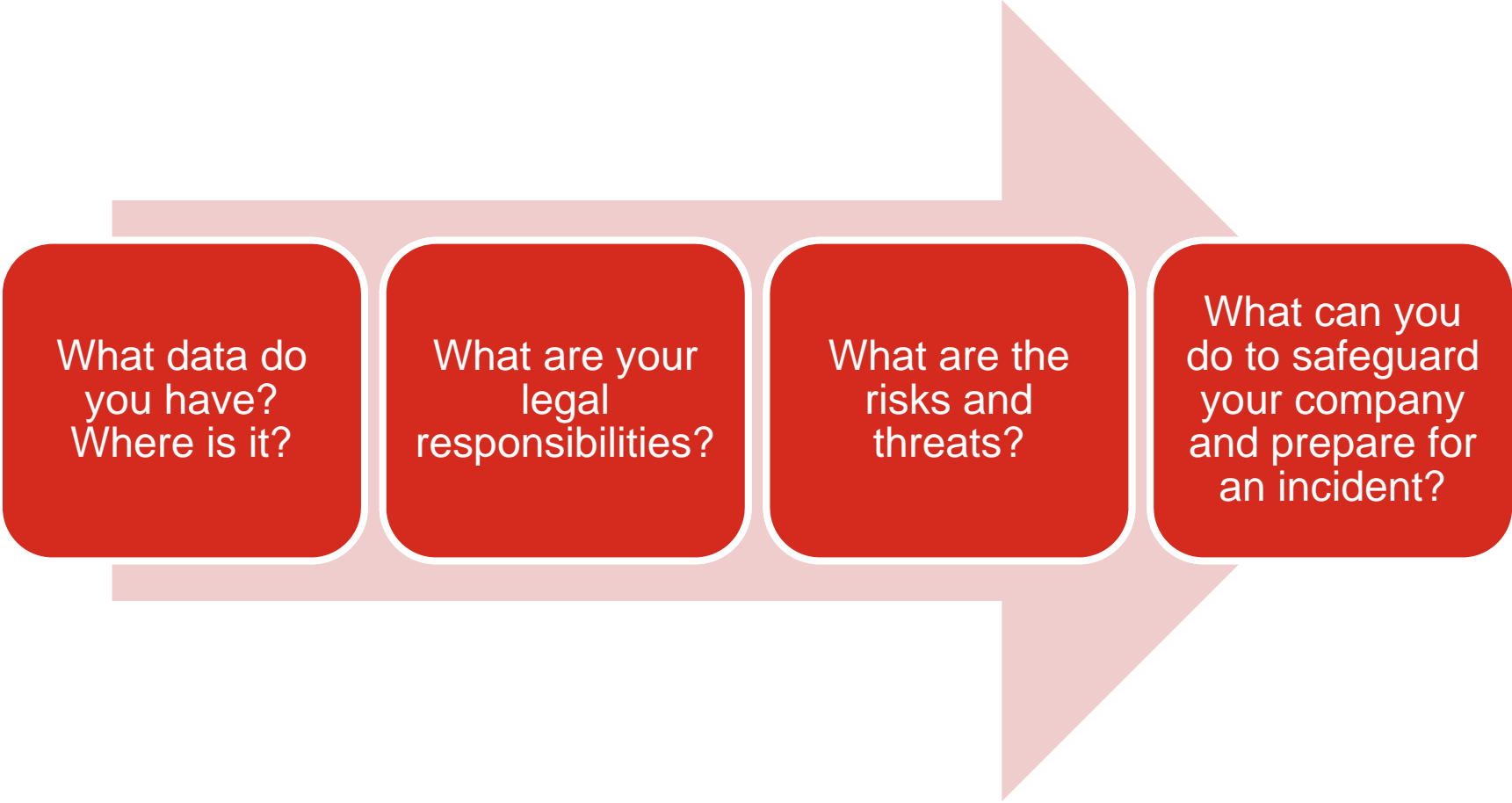
Target Is Not Alone

- Home Depot (2014) – 56 million customer email addresses and payment cards
- JPMorgan Chase (2014) – 76 million customer names, phone numbers, and other information
- Sony (2014) – **unknown number** of files of personal information, internal Sony discussions, and unreleased films:
 - 1555 servers and 3262 PCs completely erased
 - Hackers gained access through a “spearphishing” email sent to an employee who clicked on an attachment or link
- Adobe (2013) – 152 million customer names, passwords, credit card information
- Tricare (2011) – 4.9 million medical records lost

Pop Quiz – Which of the Following Has Your Company Done?

- Prepared an information/data security policy?
- Trained your employees in data security practices?
- Conducted an audit or assessment of cyber threat preparedness?
- Prepared a data breach incident response plan?
- Responded to a data breach incident?
- Does your company involve lawyers in proactive and/or reactive measures to cybersecurity?

Where to Start?



What data do you have?
Where is it?

What are your legal responsibilities?

What are the risks and threats?

What can you do to safeguard your company and prepare for an incident?

Understand Data Security and Privacy Legal and Compliance Obligations

- What laws and regulations apply?
 - No comprehensive federal legislation YET but:
 - HIPAA
 - Gramm-Leach-Bliley Act
 - Section 5 of the FTC Act
 - State laws
- Is your organization in compliance with those laws and regulations?
- Are you prepared to follow the applicable laws and regulations in the event of a breach or other incident?

Federal Trade Commission Act, Section 5

- Section 5 gives the FTC authority to investigate “unfair or deceptive acts or practices in or affecting commerce,” including data security and privacy practices
- FTC guidance:
 - Adopt a “privacy by design” strategy:
 - Incorporate privacy protections into practices
 - Maintain comprehensive data management procedures
 - Offer simplified choices for consumers about their data
 - Allow greater transparency of practices
- *FTC v. Wyndham* (3d Cir. Aug. 24, 2015) – confirms that the FTC has authority to regulate cybersecurity under the “unfairness” prong

Pending Federal Legislation

In October 2015, the Cybersecurity Information Sharing Act (CISA) passed the Senate with a vote of 74 to 21.

- CISA would create a single system that sends cyber threat indicators to DHS, which would share with other government agencies and participating companies.
- CISA would eliminate liability related to the sharing of information about cyber threats with the government.
- Privacy guards would require that companies wipe customer data before sharing with the government.

Must now be merged with two bills that passed in the House.

Tennessee

Tenn. Code Ann. §§ 47-18-2105 to
-2107 (2005)

- Applies to any person or entity doing business in Tennessee that maintains electronic data containing personal information
- Notification to impacted individuals required when breach occurs
- Timing = must be in the most expedient time possible and without reasonable delay

TN Department of Safety and
Homeland Security cyber
awareness resources at
[http://www.tn.gov/safety/topic/cyber
awareness](http://www.tn.gov/safety/topic/cyber-awareness):

- Description of frauds, threats, and scams
- Monthly newsletter
- Cyber Safety Tips
- Cyber Reference Aid

Public Companies Must Understand Disclosure Obligations

- **SEC Disclosure Guidance (2011)** on disclosure of cybersecurity risks and cyber incidents
 - **In Risk Factors** – if the risk of cyber incidents is among the most significant factors that makes investment speculative or risky
 - **In Management’s Discussion of Financial Condition and Results of Operations** – if costs or the risk of incidents represent a material event or are reasonably likely materially affect results
 - **In Legal Proceedings** – if there is a material cyber-related proceeding
 - **In Financial Statements** – if cyber incidents affect line items or require special accounting treatment
 - **In Disclosure Controls and Procedures** – if cyber incidents risk the company’s ability to record or report information required to be disclosed and there are deficiencies in disclosure controls

Serve as Counsel to Your Information Technology, Risk Management and Senior Management Teams

- Be familiar with who in your organization is involved – Board of Directors, Senior Management, Records Management and Information Governance, Human Resources, Information Technology and Network Administration, Legal Department or General Counsel.
 - Be prepared to advise and counsel these functions as to legal and regulatory issues and questions.
 - Provide updates on evolving laws, regulations, and enforcement activities.
- Accountability – who is primarily responsible? Chief Security Officer or Chief Information Security Officer?
- Board and management set the tone from the top.

What Are the Standards for Securing Data?

- Other than financial, health, and payment information, there generally are not mandatory standards.
- Consider adopting and documenting your own data security policies.
 - National Institute of Standards and Technology (NIST) offers guidelines
 - Cybersecurity risk insurance policies also can help guide
 - Many require the insured to follow “minimum required practices” listed in a policy endorsement to ensure network security
 - ISO27001 technology standard for an information security management system (International Organization for Standardization)
 - ISO27002 provides best practice recommendations for information security management

NIST's Cybersecurity Framework

- In February 2013, President Obama issued Executive Order 13636, directing NIST to develop a cybersecurity framework.
- In February 2014, NIST published its Cybersecurity Framework, a set of industry standards and best practices to help organizations manage cybersecurity risks.
 - Framework Core Functions:
 - Identify systems, data, capabilities
 - Protect critical infrastructure by developing safeguards
 - Detect cybersecurity events by monitoring and testing
 - Respond to events to contain and manage impact
 - Recover capabilities and systems after an event

NIST Cybersecurity Resources:

Industry resources on NIST's website:

- Case studies
- Industry guidance – examples:
 - FDA's guidance on Cybersecurity in Medical Devices
 - Conference of State Bank Supervisors' Resource Guide for Bank Executives
 - National Association of Corporate Directors' Cyber-Risk Oversight Handbook
- Assessment tools – examples:
 - FFIEC's Cybersecurity Assessment Tool
 - University of Maryland Supply Chain Management Center's CyberChain Portal-Based Assessment Tool

<http://www.nist.gov/cyberframework/cybersecurity-framework-industry-resources.cfm>

C³ Voluntary Program

- In February 2014, Department of Homeland Security released the **C³ Voluntary Program** to help connect organizations using the Cybersecurity Framework to government and private resources:
 - Cyber Resilience Reviews
 - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at <https://ics-cert.us-cert.gov/>
 - Resources include:
 - Advanced Analytical Laboratory – incident response activities
 - Outreach and training courses
 - Cybersecurity Evaluation Tool
 - National Cyber Awareness System (NCAS) – publishes information about security threats and topics

Key Records Management Principles:

Understand what you have, so that you can protect it.

If you do not need data, you should not retain it, but you must ensure that your data retention and destruction policies are defensible.

What retention obligations do you have?

Case Study – BJ’s Wholesale Club

BJ’s collected customers’ credit and debit card information to process transactions.

- BJ’s failed to encrypt and continued to store the data for 30 days.
- Hackers stole the account data and used it to make counterfeit credit and debit cards.

FTC filed a complaint under Section 5.

Settlement – BJ’s must establish a comprehensive data security program, comply with standard recordkeeping requirements, and obtain third-party security assessments biennially for 20 years.

Lesson learned – Do not retain information once you no longer have a legitimate need for it!

Case Study – Rite Aid and CVS

FTC investigations followed reports that the companies were disposing of trash containing pharmacy labels and job applications in open dumpsters.

Rite Aid had told customers that it “takes its responsibility for maintaining your protected health information in confidence very seriously.”

Settlement – Companies must establish a comprehensive data security program and obtain third-party security assessments biennially for 20 years.

Lesson learned – Dispose of sensitive data securely!

Records Management Questions

- **Are you retaining data longer than necessary?**
- **Are your personnel aware of policies?**
 - For data retention?
 - For data security?
- **Where is your email and other data stored?**
 - Shared drives? SharePoint sites? Content management systems?
 - Archives?
 - Printed hard copies?
- **What activity is happening outside your firewall?**
 - Saving to flash drives or DVDs
 - Saving to laptops or tablets
 - Saving to cloud storage
 - Forwarding to personal email account

Identify the Risks, Threats and Vulnerabilities

- Employee and contractor risks – accidental or rogue loss or theft of information
 - Trade secret information, intellectual property
 - For public companies, insider financial and other information
 - Personal information about employees and/or clients
 - Strategic information
- Vendor management and outsourcing
- Mobile platforms such as laptops and PDAs
- Poor controls
- Wrongful use or collection of information
- Cyberattacks, hacks, and scams – such as phishing

Case Study – Twitter

FTC 2010 complaint alleged that Twitter granted most employees administrative rights, including to reset user account passwords, view nonpublic tweets, and send tweets on users' behalf.

- Increased the risk that a compromise of any of its employees' credentials could result in a serious breach.
- 2010 Settlement – Twitter must establish a comprehensive data security program and obtain third-party security assessments biennially for 10 years.

Lesson learned – limit employees' access to your system's administrative controls to those with job needs!

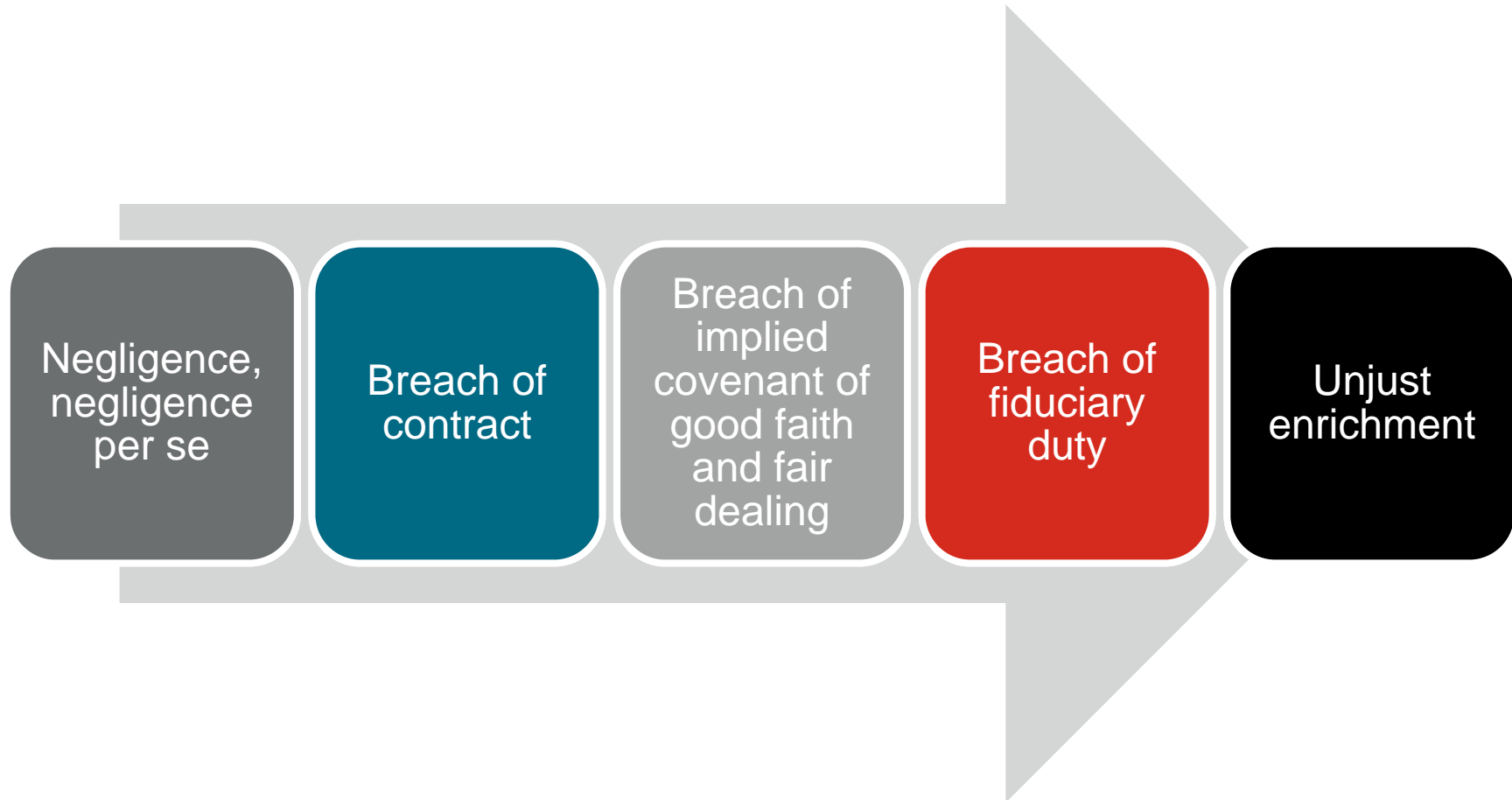
What Are the Emerging Trends?

- **Georgia Tech 2016 Emerging Cyber Threats Report:**
 - Businesses are collecting more data = risk to privacy
 - Visits to the top 100 websites are tracked by 1300+ firms
 - Shortfall in skilled IT security personnel
 - Shortfall of 1.5 million workers by 2020
 - Growth of the “Internet of Things” (connected consumer and industry devices and sensors) will grow to between 25 and 50 billion devices by 2020
 - Information theft and espionage
 - 2014 U.S. Office of Personnel Management breach
 - 2014 Sony Pictures hack

A Quick Note About Social Media Risks:

- Beware employees' inadvertent disclosures of confidential business information:
 - Example #1 – Buyer's M&A team member posted social media messages about due diligence field trip; competitor discovered identity of the target company.
 - Example #2 – Executive at HP inadvertently revealed details of a cloud-computing initiative to HP's rivals when he described it on his LinkedIn profile.
 - Example #3 – VP's LinkedIn status update warned of impending company bankruptcy six months before the company filed.

Litigation Risks – What Are the Theories of Liability?



Develop, Implement, and Update Your Program

- Identify the team.
- Identify and document controls, practices, policies and procedures.
- Conduct a risk assessment – understand your existing controls and what is missing.
- Conduct a business impact analysis.
- Develop a data incident response plan.
- Implement controls (administrative, physical, and technical) to address risk, prioritize based on business impact analysis.
- Train your personnel.
- Test and retest.
- Improve and modify your risk management program as you identify vulnerabilities.

Case Study – Fandango

Fandango's mobile app disabled SSL encryption, which would have verified that the app's communications were secure.

- Audits did not assess whether transmissions of information were secure.

A researcher contacted Fandango about the failure to validate SSL certificates, but Fandango's system categorized the report as a password reset request.

Fandango learned about the vulnerability from FTC staff.

Lesson learned – Test, audit, and assess for vulnerabilities!

Lesson learned – Have an effective process in place to receive and address security vulnerability reports!

External Dependency Management

Vendor and third-partner connectivity

Due diligence on vendors and partners

- Due diligence on their vendors and partners?
- Contracting issues

Continued audits and review of controls

Case Study – Upromise

Upromise hired a vendor to develop a browser toolbar, which collected customers' browsing history and was supposed to remove personally identifying information (PII).

- Vendor's toolbar collected PII and transmitted it in clear text.

FTC filed a complaint in 2012.

Settlement – Upromise must disclose its data collection practices, obtain consumers' consent for any toolbar products and how to disable them, and obtain biennial independent security assessments for the next 20 years.

Lesson learned – ask questions and verify that your vendors comply with your privacy and security policies and your contracts with them!

Insure Against Cyber Risks

- Don't assume you are covered under general liability policies
- Cyber coverage – what is typically covered?
 - First party vs. third party losses
 - Business interruption as a result of network or web site outage
 - Costs from comprised digital assets
 - Cyber extortion – threats to post/sell security vulnerabilities and/or confidential data - including ransomware
 - Theft or destruction of trade secrets
 - Breach notification and mitigation
 - Reputational loss

Be Prepared to Handle Breaches and Other Incidents

- Preparation is key.
 - Document the plan.
 - Know the plan.
 - Train on the plan.
 - Test the plan.
- Are the team members identified and ready?
 - Who from the legal team will be involved with the response team?
 - Do you have a forensic team lined up?
 - Do you have internal and/or external PR personnel on board?
- Are you covered by insurance? Know your insurance coverage!

Cyber Incident Response Checklist

- Identify your team – internal team plus external vendors and advisors.
- Understand your systems and data.
- Decide whether notification is required under any applicable laws or regulations (and if so, what are the deadlines for notification).
- Decide whether you have a duty to self-report and/or cooperate with law enforcement and regulators.
- Know your plan – what steps are you going to take and who is going to be responsible for each step.
- Determine your message – communications and reputation management.
- Decide what remediation is required (such as credit monitoring).

Questions?

Mark Glover

Shareholder

901.577.2222

mglover@bakerdonelson.com

George T. (Buck) Lewis

Shareholder

901.577.2256

blewis@bakerdonelson.com

Angie Davis

Shareholder

901.577.8110

angiedavis@bakerdonelson.com

Kristine Roberts

Shareholder

901.577.8136

klroberts@bakerdonelson.com